PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference GIC-564 PCT	**FOR FURTHER ACTION** see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
International application No. PCT/US 00/01021	International filing date *(day/month/year)* 14/01/2000	(Earliest) Priority Date *(day/month/year)* 22/01/1999
Applicant GENERAL INSTRUMENT CORPORATION et al.		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 3 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

□ the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing :

□ contained in the international application in written form.

□ filed together with the international application in computer readable form.

□ furnished subsequently to this Authority in written form.

□ furnished subsequently to this Authority in computer readble form.

□ the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

□ the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. □ **Certain claims were found unsearchable** (See Box I).

3. □ **Unity of invention is lacking** (see Box II).

4. With regard to the **title,**

☒ the text is approved as submitted by the applicant.

□ the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**

☒ the text is approved as submitted by the applicant.

□ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No. 2

☒ as suggested by the applicant.

□ because the applicant failed to suggest a figure.

□ because this figure better characterizes the invention.

□ None of the figures.

International Application No
PCT/US 00/01021

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/173 H04N17/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N H04B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 335 265 A (SONBERG KENNETH W ET AL) 2 August 1994 (1994-08-02) column 1, line 59 -column 2, line 21 column 8, line 27 - line 61 table 1 figures 1-4 ---	1-3,7, 24,25
A	ELDERING C A ET AL: "CATV RETURN PATH CHARACTERIZATION FOR RELIABLE COMMUNICATIONS" IEEE COMMUNICATIONS MAGAZINE,US,IEEE SERVICE CENTER. PISCATAWAY, N.J, vol. 33, no. 8, 1 August 1995 (1995-08-01), pages 62-69, XP000525541 nEW yORK, ny, us ISSN: 0163-6804 --- -/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 28 April 2000	Date of mailing of the international search report 08/05/2000
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Van der Zaal, R

1

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 473 361 A (PENNEY BRUCE J) 5 December 1995 (1995-12-05) -----	

1

ormation on patent family members

ternational Application No

PCT/US 00/01021

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5335265 A	02-08-1994	DE 69227122 D	29-10-1998
		DE 69227122 T	25-03-1999
		EP 0611513 A	24-08-1994
		JP 7500955 T	26-01-1995
		WO 9309640 A	13-05-1993
US 5473361 A	05-12-1995	NONE	

ATENT COOPERATION TREA

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To: BARRY LIPSITZ
755 MAIN STREET
BUILDING NO. 8
MONROE, CT 06468

PCT

WRITTEN OPINION

(PCT Rule 66)

Date of Mailing (*day/month/year*) 10 MAY 2001

Applicant's or agent's file reference
GIC-564PCT

REPLY DUE within TWO months from the above date of mailing

International application No. PCT/US00/01021	International filing date (*day/month/year*) 14 JANUARY 2000	Priority date (*day/month/year*) 22 JANUARY 1999

International Patent Classification (IPC) or both national classification and IPC
IPC(7): H04N 7/167 and US Cl.: 348/12 ; 380/20

Applicant
GENERAL INSTRUMENT CORPORATION

1. This written opinion is the first (first, etc.) drawn by this International Preliminary Examining Authority.

2. This opinion contains indications relating to the following items:

I ☒ Basis of the opinion

II □ Priority

III □ Non-establishment of opinion with regard to novelty, inventive step or industrial applicability

IV □ Lack of unity of invention

V ☒ Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

VI ☒ Certain documents cited

VII □ Certain defects in the international application

VIII □ Certain observations on the international application

3. The applicant is hereby invited to reply to this opinion.

When? See the time limit indicated above. ~~The applicant may, before the expiration of that time limit, request this Authority to grant an extension., see Rule 66.2(d).~~

How? By submitting a written reply, accompanied, where appropriate, by amendments, according to Rule 66.3. For the form and the language of the amendments, see Rules 66.8 and 66.9.

Also For an additional opportunity to submit amendments, see Rule 66.4.
For the examiner's obligation to consider amendments and/or arguments, see Rule 66.4 *bis*.
For an informal communication with the examiner, see Rule 66.6.

If no reply is filed, the international preliminary examination report will be established on the basis of this opinion.

4. The final date by which the international preliminary examination report must be established according to Rule 69.2 is: 22 MAY 2001.

Name and mailing address of the IPEA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
ANDREW FAILE
Telephone No. (703) 3[illegible]-2399

WRITTEN OPINION

International application No.

PCT/US00/01021

I. Basis of the opinion

1. With regard to the **elements** of the international application:*

□ the international application as originally filed

☒ the description:

pages 1-22, as originally filed

pages NONE, filed with the demand

pages NONE, filed with the letter of ______

☒ the claims:

pages 23-27, as originally filed

pages NONE, as amended (together with any statement) under Article 19

pages 28, filed with the demand

pages NONE, filed with the letter of ______

☒ the drawings:

pages 1-5, as originally filed

pages NONE, filed with the demand

pages NONE, filed with the letter of ______

☒ the sequence listing part of the description:

pages NONE, as originally filed

pages NONE, filed with the demand

pages NONE, filed with the letter of ______

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language ______ which is:

□ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

□ the language of publication of the international application (under Rule 48.3(b)).

□ the language of the translation furnished for the purposes of international preliminary examination (under Rules 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the written opinion was drawn on the basis of the sequence listing:

□ contained in the international application in printed form.

□ filed together with the international application in computer readable form.

□ furnished subsequently to this Authority in written form.

□ furnished subsequently to this Authority in computer readable form.

□ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

□ The statement that the information recorded in computer readable form is identical to the writen sequence listing has been furnished.

4. ☒ The amendments have resulted in the cancellation of:

☒ the description, pages NONE

☒ the claims, Nos. NONE

☒ the drawings, sheets/~~fig~~ NONE

5. □ This opinion has been drawn as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this opinion as "originally filed".*

WRITTEN OPINION

International application No.
PCT/US00/01021

V. Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. statement

Novelty (N)	Claims	2, 5 & 15-22	YES
	Claims	1, 3-4, 6-14 & 23-25	NO
Inventive Step (IS)	Claims	NONE	YES
	Claims	1-25	NO
Industrial Applicability (IA)	Claims	1-25	YES
	Claims	NONE	NO

2. citations and explanations

Claims 1, 3-4, 6-14 & 23-25 lack novelty under PCT Article 33(2) as being anticipated by Bednarek, (U.S. Pat # 5,621,793).

Considering claims 1, 24 & 25, the claimed method, apparatus & means for detecting a clone subscriber unit in a communication network, comprising the steps of recording transmission characteristics of a signal from an original subscriber unit that is authorized for the network and measuring a comparable transmission characteristic of a signal from a subscriber unit attempting to access services from the instant network; determining whether there is a difference between the measured characteristic & the recorded characteristic, such that if there is a difference, that the subscriber unit attempting to access services from the network is identified as a clone, reads on the disclosure of Bednarek, (Abstract; col. 1, lines 55-60; col. 2, lines 5-12; col. 3, lines 48-51; col. 10, lines 1-15). In particular, Bednarek teaches determining the validity of subscriber unit, based on whether the detected time delay of messages from the instant subscriber unit is in accordance with the expected time delay from the particular subscriber unit.

Considering claim 3, the time delay characteristic measured in Bednarek is associated with the physical layer of the network.

Considering claims 4 & 6, Bednarek is applicable to wireless, as well as cable networks, (col. 1, lines 10-30.

Considering claims 7-10, see Bednarek col. 10, lines 1-15.

Considering claims 11-14, Bednarek teaches that the detection of the time delay is performed utilizing a clock within the subscriber terminal equipment, which may contain a time bias or offset, (col. 10, lines 23-50). Moreover, Bednarek teaches utilizing multiple algorithms for confirming the veracity of a detected position of a subscriber terminal equipment, which reads on a second resolution of data.

(Continued on Supplemental Sheet.)

WRITTEN OPINION

International application No.
PCT/US00/01021

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: Boxes I - VIII

Sheet 10

TIME LIMIT:

The time limit set for response to a Written Opinion may not be extended. 37 CFR 1.484(d). Any response received after the expiration of the time limit set in the Written Opinion will not be considered in preparing the International Preliminary Examination Report.

V. 2. REASONED STATEMENTS - CITATIONS AND EXPLANATIONS (Continued):

Considering claim 23, see Bednarek col. 10, lines 9-40.

Claims 2, 5 & 15-22 lack an inventive step under PCT Article 33(3) as being obvious over Bednarek.

Considering claim 2, Bednarek teaches that the recording, measuring and determining may be performed at the subscriber units, (col. 7, lines 23-35; col. 8, lines 25-30. Official Notice is taken at the time the invention was made, it was well known in the art to process complicated algorithms at a central location, remote from a subscriber unit. It would have been obvious for one of ordinary skill in the art at the time the invention was made, to modify Bednarek with the well known technique of utilizing the processing capacity at the headend, at least for the desirable benefit of avoiding the need f or costly processors in subscriber terminal equipment, thereby reducing the cost of such equipment.

Considering claim 5, even though Bednarek does not discuss the use of cable modems within subscriber terminal equipment, Official Notice is taken that such a feature was well known in the art at the time the invention was made. It would have been obvious for one of ordinary skill in the art at the time the invention was made, to modify Bednarek with the well known technique of utilizing cable modems within a subscriber terminal equipment, at least for the desirable benefit of flexibility in the types of transmission formats the instant subscriber terminal equipment is enabled to receive.

Considering claims 15-22, Official Notice is taken that at the time the invention was made, it was well known in the art of remote diagnostic testing, to monitor, measure & detect various operating characteristics of a subscriber's terminal equipment, such as its operating channel frequency, operating power level, and power spectrum. It would have been obvious for one of ordinary skill in the art at the time the invention was made, to modify Bednarek with the well known technique of remote diagnostics, for the desirable advantage of a more accurate & reliable determination of whether or not a particular subscriber terminal under test, is in fact a clone, or a valid terminal.

-------------------- NEW CITATIONS --------------------

US 5,621,793 A (BEDNAREK, et al) 15 April 1997; Abstract; col. 10, lines 1-45.

US 4,829,589 A (UEKUSA) 09 May 1989; Abstract.

US 4,688,249 A (HAYES, et al) 18 August 1987; Abstract.

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Assistant Commissioner for Patents
United States Patent and Trademark
Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 06 October 2000 (06.10.00)	
International application No. PCT/US00/01021	**Applicant's or agent's file reference** GIC-564 PCT
International filing date (day/month/year) 14 January 2000 (14.01.00)	**Priority date** (day/month/year) 22 January 1999 (22.01.99)
Applicant ANDERSON, Steven, E.	

1. The designated Office is hereby notified of its election made:

☒ in the demand filed with the International Preliminary Examining Authority on:

25 July 2000 (25.07.00)

□ in a notice effecting later election filed with the International Bureau on:

____

2. The election ☒ was

□ was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer Claudio Borton
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

09/889540 (ZFC1)

14

9889.540

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference GIC-564PCT	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/US00/01021	International filing date *(day/month/year)* 14 JANUARY 2000	Priority date *(day/month/year)* 22 JANUARY 1999
International Patent Classification (IPC) or national classification and IPC IPC(7): H04N 7/167 and US Cl.: 725/121; 348/12 ; 380/20		
Applicant GENERAL INSTRUMENT CORPORATION		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets.

   □ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority. (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of ______ sheets.

3. This report contains indications relating to the following items:

   I ☒ Basis of the report

   II □ Priority

   III □ Non-establishment of report with regard to novelty, inventive step or industrial applicability

   IV □ Lack of unity of invention

   V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

   VI □ Certain documents cited

   VII □ Certain defects in the international application

   VIII □ Certain observations on the international application

Date of submission of the demand 25 JULY 2000	Date of completion of this report 30 AUGUST 2001
Name and mailing address of the IPEA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer ANDREW FAILE Telephone No. (703) 305-2399

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/US00/01021

I. Basis of the report

1. With regard to the elements of the international application:*

□ the international application as originally filed

☒ the description:
pages 1-22, as originally filed
pages NONE, filed with the demand
pages NONE, filed with the letter of ______

☒ the claims:
pages 23-28, as originally filed
pages 28, as amended (together with any statement) under Article 19
pages NONE, filed with the demand
pages NONE, filed with the letter of ______

☒ the drawings:
pages 1-5, as originally filed
pages NONE, filed with the demand
pages NONE, filed with the letter of ______

☒ the sequence listing part of the description:
pages NONE, as originally filed
pages NONE, filed with the demand
pages NONE, filed with the letter of ______

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language ______ which is:

□ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

□ the language of publication of the international application (under Rule 48.3(b)).

□ the language of the translation furnished for the purposes of international preliminary examination (under Rules 55.2 and/ or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

□ contained in the international application in printed form.

□ filed together with the international application in computer readable form.

□ furnished subsequently to this Authority in written form.

□ furnished subsequently to this Authority in computer readable form.

□ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

□ The statement that the information recorded in computer readable form is identical to the writen sequence listing has been furnished.

4. ☒ The amendments have resulted in the cancellation of:

☒ the description, pages NONE
☒ the claims, Nos. NONE
☒ the drawings, sheets/~~fig~~ NONE

5. □ This report has been drawn as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17).*

***Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. **statement**

Novelty (N)	Claims	2, 5 & 15-22	YES
	Claims	1, 3-4, 6-14 & 23-25	NO
Inventive Step (IS)	Claims	NONE	YES
	Claims	1-25	NO
Industrial Applicability (IA)	Claims	1-25	YES
	Claims	NONE	NO

2. **citations and explanations (Rule 70.7)**

Response to Arguments

Applicant's arguments filed 14 JUNE 2001 have been fully considered, but are not persuasive.

On page 2 of the response, applicant argues that "the subscriber unit transmits a signal to the detection apparatus. Based on this signal, a determination is made (e.g. at the CATV headend...)". Examiner agrees with this statement, however it is noted that only claim 2 requires that the "recording, measuring and determining steps occur at the headend".

Applicant argues further on page 2, that "a transmission characteristic of a signal from an original subscriber unit is recorded" is to be interpreted that a subscriber unit(s) transmit the signals from which the 'transmission' characteristics are measured". It is agreed that that is one possible meaning of the claim. Nevertheless, examiner asserts that "recording a transmission characteristic of a signal *from a* subscriber unit..", also reads on a transmission characteristic of a signal *at a* subscriber unit, or *with respect to* a subscriber unit.. The independent claims **do not recite** that the transmission characteristic is of a signal from a subscriber unit, to the headend, or to any other remote device. The independent claims merely recite that the transmission characteristics are from a subscriber unit.

Therefore the claims only require that the transmission characteristic relate to the instant subscriber unit. In otherwords, since in Bednarek the measured distance and time delay are transmission characteristics *from the* instant subscriber unit, the reference meets the limitations of the claimed subject matter. Transmission characteristic is broad enough to read on the parameters of transmission parameters of the network with respect to a particular subscriber unit. Thus, (Continued on Supplemental Sheet.)

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: Boxes I - VIII **Sheet 10**

V. 2. REASONED STATEMENTS - CITATIONS AND EXPLANATIONS (Continued):
since different subscriber units will use networks, they will have different transmsission parameters.

It is asserted that claim 2 which recites that the "recording, measuring and determining steps occur at the headend", would have been an obvious modification of Bednarek. The instant reference discloses that security of the set top box is a problem which may be solved by various tamper-proof algorithms see col. 13 & col. 14. Clearly, one of ordinary skill in the art would have also recognized the benefit of employing measuring and determining hardware and software remote from set top boxes, at least for the known security feature of avoiding persons local to the set top box with tampering with the instant determining means.

Analysis of Claims

Claims 1, 3-4, 6-14 & 23-25 lack novelty under PCT Article 33(2) as being anticipated by Bednarek, (U.S. Pat # 5,621,793).

Considering claims 1, 24 & 25, the claimed method, apparatus & means for detecting a clone subscriber unit in a communication network, comprising the steps of recording transmission characteristics of a signal from an original subscriber unit that is authorized for the network and measuring a comparable transmission characteristic of a signal from a subscriber unit attempting to access services from the instant network; determining whether there is a difference between the measured characteristic & the recorded characteristic, such that if there is a difference, that the subscriber unit attempting to access services from the network is identified as a clone, reads on the disclosure of Bednarek, (Abstract; col. 1, lines 55-60; col. 2, lines 5-12; col. 3, lines 48-51; col. 10, lines 1-15). In particular, Bednarek teaches determining the validity of subscriber unit, based on whether the detected time delay of messages from the instant subscriber unit is in accordance with the expected time delay from the particular subscriber unit.

Considering claim 3, the time delay characteristic measured in Bednarek is associated with the physical layer of the network.

Considering claims 4 & 6, Bednarek is applicable to wireless, as well as cable networks, (col. 1, lines 10-30.

Considering claims 7-10, see Bednarek col. 10, lines 1-15.

Considering claims 11-14, Bednarek teaches that the detection of the time delay is performed utilizing a clock within the subscriber terminal equipment, which may contain a time bias or offset, (col. 10, lines 23-50). Moreover, Bednarek teaches utilizing multiple algorithms for confirming the veracity of a detected position of a subscriber terminal equipment, which reads on a second resolution of data.

Considering claim 23, see Bednarek col. 10, lines 9-40.

Claims 2, 5 & 15-22 lack an inventive step under PCT Article 33(3) as being obvious over Bednarek.

Considering claim 2, Bednarek teaches that the recording, measuring and determining may be performed at the subscriber units, (col. 7, lines 23-35; col. 8, lines 25-30. Official Notice is taken at the time the invention was made, it was well known in the art to process complicated algorithms at a central location, remote from a subscriber unit. It would have been obvious for one of ordinary skill in the art at the time the invention was made, to modify Bednarek with the well known technique of utilizing the processing capacity at the headend, at least for the desirable benefit of avoiding the need for costly processors in subscriber terminal equipment, thereby reducing the cost of such equipment.

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: Boxes I - VIII

Sheet 11

Considering claim 5, even though Bednarek does not discuss the use of cable modems within subscriber terminal equipment, Official Notice is taken that such a feature was well known in the art at the time the invention was made. It would have been obvious for one of ordinary skill in the art at the time the invention was made, to modify Bednarek with the well known technique of utilizing cable modems within a subscriber terminal equipment, at least for the desirable benefit of flexibility in the types of transmission formats the instant subscriber terminal equipment is enabled to receive.

Considering claims 15-22, Official Notice is taken that at the time the invention was made, it was well known in the art of remote diagnostic testing, to monitor, measure & detect various operating characteristics of a subscriber's terminal equipment, such as its operating channel frequency, operating power level, and power spectrum. It would have been obvious for one of ordinary skill in the art at the time the invention was made, to modify Bednarek with the well known technique of remote diagnostics, for the desirable advantage of a more accurate & reliable determination of whether or not a particular subscriber terminal under test, is in fact a clone, or a valid terminal.

Claims 1, 24-25 lack novelty under PCT Article 33(2) as being anticipated by Rangedahl, (U.S. Pat # 5,790,074).

Considering claims 1, 24 & 25, the claimed method, apparatus & means for detecting a clone subscriber unit in a communication network, comprising the steps of recording transmission characteristics of a signal from an original subscriber unit that is authorized for the network and measuring a comparable transmission characteristic of a signal from a subscriber unit attempting to access services from the instant network; determining whether there is a difference between the measured characteristic & the recorded characteristic, such that if there is a difference, that the subscriber unit attempting to access services from the network is identified as a clone, reads on the disclosure of Rangedahl which teaches that a user device 10 transmits an authorization request to a centralized authorization device 20. In Rangedahl, the user device 10 authorization request includes the GPS data of the instant user device 10. The authorization device 20 receives the GPS and determines whether the received GPS matches the known position of the identified reciver.

<u>Additional Citations</u>

Laurance is also cited since it is relevant to applicant's claims. The system of Laurance discloses the very well known technique of authenticating a transmission device as a function of its location, (Fig. 1; col. 5, lines 8-20; col. 13, lines 14-21). The location of the device, i.e distance from the centralized authorization device. reads on the claimed transmisssion characteristics. Likewise, MacDoran teaches determining the location of a receiver device in order to avoid spoofing.

------------------- NEW CITATIONS -------------------

US 5,621,793 A (BEDNAREK, et al) 15 April 1997; Abstract; col. 10, lines 1-45.

US 4,829,589 A (UEKUSA) 09 MAY 1989; Abstract.

US 4,688,249 A (HAYES, et al) 18 AUGUST 1987; Abstract.

US 5,790,074 A (RANGEDAHL, et al) 04 AUGUST 1998. Abstract; col. 2, lines 22-32; col. 5, lines 58-67.

US 4,860,352 A (LAURANCE, et al) 22 AUGUST 1989. Abstract; col. 13, lines 12-25.

US 5,757,916 A (MacDORAN, et al) 26 MAY 1998. Abstract; col. 9, lines 54-65.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference GIC-564 PCT	**FOR FURTHER ACTION** see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
International application No. PCT/US 00/ 01021	International filing date *(day/month/year)* 14/01/2000	(Earliest) Priority Date *(day/month/year)* 22/01/1999
Applicant GENERAL INSTRUMENT CORPORATION et al.		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 3 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

a. With regard to the **language,** the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

□ the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing :

□ contained in the international application in written form.

□ filed together with the international application in computer readable form.

□ furnished subsequently to this Authority in written form.

□ furnished subsequently to this Authority in computer readble form.

□ the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

□ the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. □ **Certain claims were found unsearchable** (See Box I).

3. □ **Unity of invention is lacking** (see Box II).

4. With regard to the **title,**

☒ the text is approved as submitted by the applicant.

□ the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**

☒ the text is approved as submitted by the applicant.

□ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No. 2

☒ as suggested by the applicant.

□ because the applicant failed to suggest a figure.

□ because this figure better characterizes the invention.

□ None of the figures.

I●ERNATIONAL SEARCH REPORT

International Application No
PCT/US 00/01021

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/173 H04N17/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N H04B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 335 265 A (SONBERG KENNETH W ET AL) 2 August 1994 (1994-08-02) column 1, line 59 -column 2, line 21 column 8, line 27 - line 61 table 1 figures 1-4 ---	1-3,7, 24,25
A	ELDERING C A ET AL: "CATV RETURN PATH CHARACTERIZATION FOR RELIABLE COMMUNICATIONS" IEEE COMMUNICATIONS MAGAZINE,US,IEEE SERVICE CENTER. PISCATAWAY, N.J, vol. 33, no. 8, 1 August 1995 (1995-08-01), pages 62-69, XP000525541 nEW yORK, ny, us ISSN: 0163-6804 --- -/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 28 April 2000	Date of mailing of the international search report 08/05/2000
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Van der Zaal, R

1

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 00/01021

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 473 361 A (PENNEY BRUCE J) 5 December 1995 (1995-12-05) -----	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 00/01021

Patent document cited in search report		Publication date	Patent family member(s)			Publication date
US 5335265	A	02-08-1994	DE	69227122	D	29-10-1998
			DE	69227122	T	25-03-1999
			EP	0611513	A	24-08-1994
			JP	7500955	T	26-01-1995
			WO	9309640	A	13-05-1993
US 5473361	A	05-12-1995	NONE			

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :
H04N 7/173, 17/00

A1

(11) International Publication Number: **WO 00/44174**

(43) International Publication Date: 27 July 2000 (27.07.00)

(21) International Application Number: PCT/US00/01021

(22) International Filing Date: 14 January 2000 (14.01.00)

(30) Priority Data:
60/116,731 22 January 1999 (22.01.99) US

(71) Applicant *(for all designated States except US)*: GENERAL INSTRUMENT CORPORATION [US/US]; 101 Tournament Drive, Horsham, PA 19044 (US).

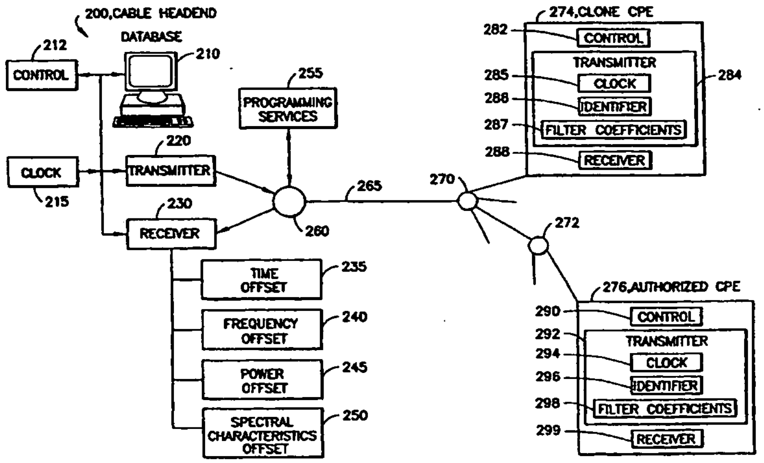
(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: ANDERSON, Steven, E. [US/US]; 5521 Taft Avenue, La Jolla, CA 92037 (US).

(74) Agent: LIPSITZ, Barry, R.; Building No. 8, 755 Main Street, Monroe, CT 06468 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
With amended claims.

(54) Title: DETECTION OF DUPLICATE PARTICIPANTS IN A TWO–WAY MODEM ENVIRONMENT



(57) Abstract

Duplicate participants (e.g., cloned subscriber units) (274) are detected in a communication network, such as a hybrid fiber/coax (HFC) cable television network or the like, by monitoring the physical layer of the network to detect transmission differences between such units. The subscriber units (14, 16, 18, 274, 276) may be cable modems that transmit upstream signals with associated identifers to a headend (10, 200), e.g., to access the Internet or for telephony. Measured characteristics of the upstream signals can include: (1) propagation time (235), (2) frequency (240), (3) power (245), and (4) spectral characteristics (250). For propagation time, the reception time of the upstream message can be compared to a headend clock (215) and also to other messages with the same modem ID. For spectral characteristics adjustment coefficients can be provided to the units to normalize the spectrum of the upstream signal to a baseline spectrum. When discrepancies are detected for an upstream signal that indicate duplicate modems are operating in the network, the account of the corresponding unit can be terminated.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

DETECTION OF DUPLICATE PARTICIPANTS IN A TWO-WAY MODEM ENVIRONMENT

BACKGROUND OF THE INVENTION

This application claims the benefit of U.S. Provisional Application No. 60/116,731, filed January 22, 1999.

The following acronyms are used:

CM - Cable Modem;

CMTS - Cable Modem Termination System;

CPE - Customer Premises Equipment;

HFC - Hybrid Fiber/Coax;

ID - Identifier;

IP - Internet Protocol; and

MAC - Medium Access Control.

The present invention relates to subscriber networks, such as HFC cable television networks, and more particularly to controlling access to services provided over the network. The invention is particularly suitable for use with networks with subscriber terminals/set-top boxes that use two-way modems, such as CMs, that are connected to the network.

Such modems are increasingly being used to allow network users to send and receive data, such as from the Internet data, at relatively high speeds. The modems may also provide telephony capabilities. The invention also is useful generally for terminals that have any upstream signaling capability via the network, e.g., to a network headend.

It is important for a network operator to control access to services that are delivered via the network. However, there is a tradeoff between the level and cost of security distributed throughout any communications network. The extremes of this tradeoff are:

(a) place all of the security within the CPE (such as in a user's home), in which case, for example, only physical security associated with encryption keys is provided; and

(b) place all of the security in the network, e.g., implement network security protocols that rely on the trust associated with the absolute identity, in this case physical location, of the distributed elements of the network.

For the latter case, if duplicate CPE could be identified with absolute certainty, security protocols and procedures can be implemented that relied on this trust. For purposes of this disclosure, the terms "consumer premises equipment", "subscriber unit", "terminal", "set-top box", "cable modem" and the like are used interchangeably.

Unauthorized persons ("pirates" or "attackers") have been successful in gaining access to networks using various attack techniques. One possible attack on a network of the type described above is to move the permanent identity of a first subscriber unit (e.g., a CM or other CPE), for which a subscriber has paid for the services provided by the network, to a second "clone" subscriber unit in the network. The first subscriber unit is known as the "clone master." This cloning can be performed if the security information or unit ID of the first subscriber unit is not protected from theft. Such cloning allows a single individual to purchase programming or other data services legitimately from the network, and then sell to others for a profit, without authorization, the ability (along with possibly modified terminals) to access the services.

An alternative motivation is the theft of the identity of a unit, then selling that identity to persons wishing to illegally use other network services and not pay. For example, current networks users who pay for a basic level of services can obtain enhanced services without paying. The network operator can incur significant revenue losses if the identity of the compromised unit were used, for example, to access long distance telephone services or gain free unlimited Internet access, e.g., via a CM.

To remain undetected in the network, the cloned unit must possess all of the characteristics of the clone master. If the clone is identical to the clone master, the clone will merely use the bandwidth and ID of the clone master. Moreover, if a clone unit has multiple (N) clone IDs, any of these identities can be used to gain access to the network. A concentration ratio of N:1 allows the cloned units to operate in the network with little chance of collision, if N is large enough.

The cloned units can continue to operate undetected if the network operator (e.g., the CMTS and associated servers operated by or for the service provider) does not detect any noticeable anomalies in the network's traffic, such as multiple IP addresses, increased traffic flows, etc. Additionally, the clones can continue to operate undetected even though the network operator verifies the identity of the unit that sends an upstream message. This is achieved because the verification of an ID of the subscriber unit (e.g., a CM or other CPE) is performed before the modem is registered with the network. The ID may specify a manufacturer's serial number, IEEE MAC address, and so forth. However, there is no practical method for any network operator to associate this address to a specific modem prior to modem registration.

A cloned network element will remain undetected as long as there are no discernable differences between any of the master and cloned units, and they operate within the network in a logical and physically possible manner.

For example, one method for detecting cloned analog cell phones is to identify telephone calls that originate from physically distant parts of the network within a short time window. However, such methods of clone detection are marginally effective at identifying cloned phones since unauthorized calls within the same general vicinity (e.g., same city) as unauthorized calls cannot be flagged. Additionally, data indicating the location, such as which network cell is used, must be communicated upstream to a central processing facility. Moreover, this technique is not easily used in a subscriber network such as an HFC cable television network since there is no provision to identify the network path (e.g., branch or hub) that is traveled by an upstream message from a clone terminal.

Accordingly, it would be advantageous to provide a reliable system for detecting cloned units, such as CMs, in a network. The system should be implementable with relatively low cost and complexity, and without significant disruptions in service. The system should recognize and take advantage of the fact that systems which support CM service or telephony service (e.g., HFC cable television and the like) allow several unique aspects of the physical layer to be exploited, such that subscriber units (e.g., modems) can be uniquely identified even if the unique ID can be cloned into other units.

The system should be compatible with the "Data Over Cable Service Interface Specification RF Interface" (DOCSIS RFI) standard.

The present invention provides a system having the above and other advantages.

SUMMARY OF THE INVENTION

The present invention provides for the detection of duplicate participants in a network having a terminal population with two-way communication capabilities by analyzing transmission differences in the physical layer of the network.

The physical layer is concerned with transmitting raw bits over a communication channel. Examples of physical layer attributes that can be used in accordance with the invention to identify a subscriber unit are unit timing offset, unit frequency offset, unit power offset, and unit spectral characteristics.

The pirate unit can continue to operate as a clone of a clone master in the network if it remains undetected. The invention determines that a cloned ID is being used by detecting differences in any detectable characteristics of the cloned subscriber unit that distinguish it from other cloned subscriber units (of the same ID) or from the cloned master.

Since the cloned units' transmissions do not all take the same upstream path in the network to the CMTS, differences in these paths present an opportunity for detecting piracy by uniquely identifying units that attempt to appear identical to the CMTS and the network. Thus, differences in the return path can be used in accordance with the invention to "tag" each unit uniquely. This approach not only relies on the assumed differences in path length, but it also relies on each of the clone modems not knowing the exact details of the corrections (adjustments) sent to the clone master.

A particular method for detecting a clone subscriber unit in a communication network, includes the step of recording a transmission characteristic of an original subscriber unit authorized for use in the network. The recorded transmission characteristic is compared to a comparable transmission characteristic of a subscriber unit on the network alleging to be the original subscriber unit. For example, the alleging unit may have the same ID in its upstream messages as the authorized unit. A difference between the compared transmission characteristics indicates that the alleging subscriber unit is a clone subscriber unit.

The observed transmission characteristic may include: (1) propagation time, (2) frequency, (3) power, and (4) spectral characteristics. For propagation time, an enhancement involves providing data for adjusting the assigned transmit time a subscriber unit at a lower resolution than the resolution at which the offset is initially determined. In this manner, even if the clone subscriber unit intercepts the offset and attempts to adjust its own transmit time accordingly, the CMTS can still detect when the transmit time offset is out of the expected range.

The enhancement can be extended to the other characteristics.

A corresponding apparatus is also presented.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of an HFC network embodying the present invention.

FIG. 2 illustrates a headend, authorized customer premises equipment (CPE), and clone CPE in a subscriber network in accordance with the present invention.

FIG. 3(a) illustrates the calculation of a signal propagation time before ranging in accordance with the present invention.

FIG. 3(b) illustrates a ranging region in accordance with the present invention.

FIG. 3(c) illustrates assigned upstream transmission slots after ranging in accordance with the present invention.

FIG. 3(d) illustrates an uncertainty region for signal propagation time in accordance with the present invention.

FIG. 4 illustrates measurement of the power spectrum of a received upstream signal at a headend in accordance with the present invention.

DETAILED DESCRIPTION OF THE INVENTION

FIG. 1 illustrates, in block diagram form, an HFC cable television plant in which the invention can be implemented. Although an HFC cable television plant is illustrated for purposes of the present disclosure, it should be appreciated that the invention can be used in other network types where the possibility of cloned CPE is a concern. A transmitter and receiver located at a cable headend 10 (i.e., service provider equipment such as a CMTS) measure one or more transmission characteristics of subscriber units 14, 16, 18 (CPE) that communicate with the headend via the network 12. Any number of subscriber units can be provided, up to the network capacity, and each can be monitored by the headend.

FIG. 2 illustrates a headend 200, authorized customer premises equipment (CPE) 276, and clone CPE 274 in a subscriber network. The cable headend 200 includes a control 212, clock 215, database 210, transmitter 220, receiver 230, and a programming services function 255. The programming services function 255 may provide television programs on the network, for example. The receiver 230 is associated with a time offset function 235, a frequency offset function 240, a power offset function 245, and a spectral characteristics offset function 250. The control 212 provides overall management of the functions at the headend 200.

The transmitter 220 transmits data via a hub 260, a network link 265, and example hubs 270 and 272 to an authorized CPE (i.e., a master unit). The transmitter transmits data via the example hubs 270 to an example clone CPE 274. Any number of clone units may be present in a network.

The clone CPE 274 includes a control 282, a transmitter 284, and a receiver 288. The transmitter 284 further includes a clock 285, an identifier (ID) function 286, and a filter with filter coefficients 287. Similarly, the authorized CPE 276 includes a control 290, a transmitter 292 (with a clock 294, an ID function 296, and a filter with filter coefficients 296), and a receiver 299.

Each of the CPE units 274, 276 can send upstream signals to, and receive signals from, the headend (or CMTS) 200. For example, if the units are CMs, the upstream signals can be for accessing the Internet, general IP-based media services or placing telephone calls. Commonly, a television, PC or other output devices are associated with each CPE unit. The data transmitted to the units 274, 276 includes data related to the service being used, along with data from the headend 200 for assigning time slots for the units to transmit upstream according to their respective bandwidth needs.

In accordance with the invention, transmission characteristics of the upstream signals are measured by the headend 200 to detect clones. These characteristics can include one or more of: (1) propagation time, (2) frequency, (3) power, and (4) spectral characteristics. Each of these is described in greater detail below.

1. In a first clone detection technique, propagation/receive time of upstream signals from the units is measured.

Generally, the ability to physically locate a subscriber unit within a network is a key factor in eliminating a timing offset attack. If the pirate can spoof the system into believing that the CPE is located in another physical location in the network, there is very little the network operator can do to locate the clone or pirate unit. This is especially true if the pirate unit is transmitting from a virtual location in the network that, to the headend, appears to be the same location as the legitimate modem.

The "Data Over Cable Service Interface Specification RF Interface" (DOCSIS RFI) specification available at www.cablemodem.com defines a network wide timestamp that is broadcast to all units which are part of the network domain. For this discussion a "domain" and a "CMTS broadcasting on a single downstream channel" are considered to be the same. The DOCSIS specification defines a periodically-transmitted message that contains a 32-bit timestamp. The least significant bit (LSB) of this timestamp is in units of 6.25 μsec/64 and is based upon a 10.24 MHz clock. The CPE modem uses this timestamp to: 1) synchronize an internal reference clock, and 2) define an exact (to within some small guard time) time to transmit on the upstream channel.

Since all of the subscriber units (e.g., 274 and 276) in the network are not the same distance from the receiver 230 in the CMTS 200, the burst arrival times of the individual subscriber units are normalized to make all of the modems appear the same virtual distance from the headend. The DOCSIS system achieves this by a process called "ranging."

FIG. 3(a) illustrates the calculation of a signal propagation time before ranging in accordance with the present invention. A time offset t1 (300) from a first cable modem, CM1, is the measured propagation time for a signal to travel from CM1 to the CMTS, and corresponds to the physical propagation distance. Similarly, a time offset t2 (310) from a second cable modem, CM2, is the measured propagation time for a signal to travel from CM2 to the CMTS.

FIG. 3(b) illustrates a ranging region in accordance with the present invention. Here, a ranging region 320 is defined for all of the CMs in the network, from the CM that is closest to the CMTS, to the CM that is farthest from the CMTS. Additionally, the CM1 has a time offset 302 for transmitting messages at t1 ±Δt1, where Δt1 is an uncertainty due to the clock rate used at the headend. Similarly, CM2 has a time offset 312 for transmitting messages at t2 ±Δt2, where Δt2 is the corresponding uncertainty.

Referring also to FIG. 2, the ranging region 320 defined within the upstream bandwidth assignment is wide enough to accommodate the closest and farthest CPE from the CMTS receiver 230. The CMTS receiver 230 measures the arrival time of the ranging burst (the burst defined to occur within this region), and determines the propagation time based on a difference between the local time, as determined by the clock 215, and an assigned upstream transmission time based on the clocks 285, 294. Clocks 285, 294 are synchronized to clock 215 via the system timestamp. The time offset is determined by a time offset function 235. The differences are then sent as a timing offset to the CPEs 274, 276 in a ranging response message and used as adjustment factors for the modem upstream transmission times.

The effect of this process is that all of the subscriber units appear to be the same virtual distance from the CMTS receiver. They actually look like they are at a zero physical distance from the CMTS upstream receiver, since the time indicated by the corrected time stamp matches the local time at the CMTS 200. Thus, the CMTS receiver knows the absolute propagation time and transmission path length of every CPE on the network within that domain. The resolution of this measurement (worst case) is approximately 100 feet, assuming a 10.24 MHz sampling clock at the CMTS receiver and using the propagation constant of electromagnetic radiation in free space (i.e., $3x10^8$ m/sec / $10.24x10^6$ Hz / 0.3048 m/ft=95.8 ft).

The propagation constants for coax cable and optical fiber are approximately 88% and 69%, respectively, of that for free space. The ratio of coax to fiber is generally known by the plant manager, but will vary greatly in different networks. Since it is not feasible to determine the exact ratio of coax to fiber in any single plant, the free space propagation constant can be used as the worst case. In addition, if the sampling rate is doubled (20.48 MHz), a worst case resolution of approximately 50 feet is achieved. Other changes in the sampling rate will affect the resolution accordingly.

FIG. 3(c) illustrates assigned upstream transmission slots after ranging in accordance with the present invention. The assigned upstream transmission slots 330 show CM1 and CM2 transmitting at the assigned times, 304 and 314, respectively, with the associated uncertainties.

FIG. 3(d) illustrates an uncertainty region for signal propagation time in accordance with the present invention. The uncertainty region 350 accounts for the uncertainties of all subscriber units (CMs) in the network, which can amount to hundreds or thousands of units. The uncertainty region width represents the worst case uncertainty based on the measurement resolution of the burst in the headend and the value of the LSB in the ranging offset sent to the CMs.

The CM1 burst 306 and CM2 burst 316 are shown as being offset from the expected receive time 340 by the corresponding uncertainties..

The ability to determine the subscriber unit distance from a known location such as a headend, and the resolution of this determination, depends primarily on the implementation of the service provider's return path receiver 230 that receives communications back from the subscriber units.

Thus, in accordance with the invention, a clone subscriber unit can be detected by measuring the propagation time of each upstream message having a given unit ID.

If the network operator determines that two different propagation times are detected from the receipt of upstream transmissions with the same ID, it can be concluded that at least one of the units is a clone. The operator can then take appropriate steps, such as terminating the account of any unit using that ID.

Accordingly, the invention allows the network operator to determine that multiple subscriber units having the same identity are present in the network. It is also possible to detect the movement of a single subscriber unit within the network.

With respect to propagation time differences, as mentioned above, the CMTS (or a comparable service provider apparatus) normalizes all of the subscriber units to appear as if they were at a zero distance from the CMTS even though they are physically located at different distances from the CMTS.

However, the above method of intrusion detection may conceivably be defeated if one could spoof the system into believing that client (subscriber) units located at different distances from the CMTS receiver were really located at the same distance from the CMTS receiver. In this case, the time offset check at the CMTS would no longer reveal cloned units. For example, assume CM1 is the clone master which has a valid network subscription, and CM2 is a clone of that modem. Note that there is additional out-of-band coordination required between clone master CMs and cloned CMs for DOCSIS transmission assignments and power control.

A clone first performs ranging as described in the previous section. However, the clone does not use its own MAC address during the initial ranging process. Instead, it uses a MAC address of some other valid CM, or possibly even some random MAC address, if the CMTS will accept it.

After this initial ranging, the clone will know its time offset from the CMTS, i.e., t2. The intrusion detection technique described earlier will not catch this clone, because it is not using its MAC address. In fact, if the clone uses a MAC address of another valid CM, an attempt at the intrusion detection could result in de-authorization of a valid CM, i.e., a denial of service attack.

After this initial ranging, the clone ranges again with the cloned MAC address. The steps are as follows:

1) CM2 (the cable modem clone) performs initial ranging using a random but valid MAC address to obtain its ranging offset, t2, from the CMTS (as illustrated earlier).

2) CM2, which has the identity (including the MAC address) of the clone master, listens for the clone master initial ranging information. Based on detecting

("snooping") the initial ranging response from the CMTS to the clone master (or through some out-of-band method), CM2 now knows the value of t1.

3) CM2 then calculates the difference between its time offset (t2) and the clone master's time offset (t1).

4) CM2 can now perform subsequent initial ranging using the clone master ID and appear to the CMTS as if it was at the same location as CM1 (the clone master). CM2 can do this by sending a ranging request t2-t1 seconds earlier than it is supposed to.

5) CM2 can now monitor ("sniff") the downstream to note any use of CM1 (or through out-of-band methods) and, if clear, CM2 can request upstream transmission slots using CM1's identity.

6) The headend sees the transmission in the correct assignment with the correct time offset and cannot tell the difference without more a sophisticated transmission arrival time detection scheme.

An advantage of this method for the attacker is that the CMTS only sees one transient ranging request with an ID that is not subscribed. All subsequent initial ranging will be performed by one of the cloned modems that are using the clone master's identity.

The intrusion detection techniques described herein can be enhanced to detect these more sophisticated attacks by increasing the frequency of the sampling clock at the CMTS (or other comparable service provider apparatus) such that a resolution of greater than, e.g., 100 feet is obtained. This provide additional ranging resolution, which may allow additional cloned units to be detected.

Another enhancement is to decrease the number of bits sent to each CPE in the ranging response time offset message, but continue to measure with the current resolution. If, for example, the granularity of the LSB is increased (e.g., by truncating the last three LSBs) the measuring resolution increases to 800 feet. The sampling frequency remains the same so the measurement resolution is still 100 feet. This technique has the effect of increasing the uncertainty of the transmission time, based upon the physical location of the modem from the cable headend CMTS and, therefore, the likelihood that duplicate CMs can be detected. This method has the disadvantage that bandwidth is sacrificed.

Alternatively, these same LSBs could be randomized and sent to each of the cloned modems. This has the additional advantage of not providing any indication to the attackers that any intrusion techniques are enabled. The uncertainty of these measurements is shown in FIG. 3(d).

2. In a second clone detection technique, frequency differences in the upstream signals from the subscriber units are used to distinguish cloned CPE units. In particular, each CPE 274, 276, transmits on an assigned center frequency. The service provider (e.g., CMTS 200) receives the transmitted signal by matching this signal's frequency and extracting the

information contained in the signal. Differences in the exact received frequency can be measured by the frequency detector 240 at the CMTS 200 or other service provider equipment to detecting duplicate units.

Optionally, adjustment data can be provided to the original subscriber unit to change its center frequency.

3. In a third clone detection technique, power differences in the upstream signals from the subscriber units are used to distinguish clone units. Each CPE 274, 276 transmits at an assigned power level. The CMTS 200 (or other service provider apparatus) sends commands to each CPE to set the power level to use for the unit's upstream transmissions. However, the power of the signal from each unit is attenuated by different amounts as the signals travel upstream in the network, so the measured level at the CMTS 200 will be less than the designated transmission levels. These decreases are a result of the differences in attenuation of the signal as the signal from each CPE traverses a different path, or part of the upstream spectrum back to the CMTS 200.

The power detector 245 at the CMTS 200 monitors each transmitted burst (upstream signal) and measures the power to determine a baseline expected power level for each unit ID. Thus, a clone unit can be identified when the measured power for a given ID does not match the expected level.

Optionally, adjustment data can be provided to the original subscriber unit to change its signal's power.

4. In a fourth clone detection technique, differences in the spectral characteristics of the upstream signals from the subscriber units are used to distinguish clone units. Each unit transmits through a unique path over the cable plant back to the service provider. The paths may cause changes in the spectral characteristics of received upstream signals.

Each burst (upstream signal) received by the CMTS 200 contains a preamble such that a demodulator (spectral characteristics detector 250) at the CMTS 200 can "train" for a period of time before the actual start of the data. During this training period, the demodulator determines the spectral characteristics of the burst and attempts to equalize the burst for optimal reception. A set of unique equalization (filter) coefficients are derived as result of the preamble spectral analysis and sent to each CM. These coefficients can also be stored in the database 210 and used to uniquely define each individual unit on the assumption that each of these units traversed a physically different path.

FIG. 4 illustrates measurement of the signal power spectrum of a received upstream signal at a headend. Using known frequency domain processing techniques, the power spectrum of a received signal might be measured as shown at 400 during the training period. The measured spectrum can be normalized to a baseline spectrum 420 using the equalization coefficients. Any significant deviation from the baseline 420 after the training period is an indication of a clone unit.

It should now be appreciated that the present invention provides techniques for locating duplicate participants (e.g., cloned subscriber units) in a communication network, such as an HFC cable television network or the like, by monitoring the physical layer of the network to detect transmission differences between such units. If such transmission differences are found from units that use a common ID, it is evident that a cloned unit is in use.

The measured characteristics can include one or more of: (1) propagation time, (2) frequency, (3) power, and (4) spectral characteristics. Moreover, a combination of characteristics can be used to provide a greater certainty that a clone exists.

Furthermore, it is not necessary to monitor each characteristic for every upstream signal. For example, only one or two characteristics need be measured. Propagation time and spectral characteristics are believed to be particularly effective in detecting clones. If a discrepancy is detected for a unit ID, the ID may be flagged as a possible clone, and other characteristics may be measured to provide a more concrete determination.

Moreover, selected unit IDs may be measured if they are suspect for some reason, such as unusually high traffic from that ID.

Random or sequential measuring of the units may also be implemented.

Moreover, the invention is not limited to use with cable modems, but may be used in any network where it is possible to measure the characteristics disclosed herein, and to relate any discrepancy to a particular unit ID.

Although the invention has been described in connection with various specific embodiments, those skilled in the art will appreciate that numerous adaptations and modifications may be made thereto without departing from the spirit and scope of the invention as set forth in the claims.

What is claimed is:

1. A method for detecting a clone subscriber unit in a communication network, comprising the steps of:

recording a transmission characteristic of a signal from an original subscriber unit that is authorized for use in said network;

measuring a comparable transmission characteristic of a signal from a subscriber unit on said network alleging to be said original subscriber unit; and

determining whether there is a difference between the measured transmission characteristic and the recorded transmission characteristic;

wherein any such difference is indicative that the alleging subscriber unit is a clone subscriber unit.

2. The method of claim 1, wherein:

said recording, measuring and determining steps occur at a headend of the network.

3. The method of claim 1, wherein:

the measured transmission characteristic is associated with a physical layer of said network.

4. The method of claim 1, wherein:

said network is a hybrid fiber/coax cable television network.

5. The method of claim 4, wherein:

said original and alleging subscriber units are cable modems.

6. The method of claim 4, wherein:

said original and alleging subscriber units comprise hybrid fiber/coax consumer premises equipment.

7. The method of claim 1, wherein:

the recorded transmission characteristic comprises at least one of a propagation time and a propagation time offset for the signal of the original subscriber unit.

8. The method of claim 7, wherein:

the propagation time offset is determined by comparing an assigned propagation time of the signal of the original subscriber unit to a receive time thereof.

9. The method of claim 7, comprising the further steps of:

providing adjustment data to adjust the propagation time offset to a desired value; and

communicating the adjustment data to any subscriber unit in the network that uses an identifier associated with the original subscriber unit for use in adjusting a propagation time offset thereof.

10. The method of claim 9, wherein:

the adjustment data is provided by a headend of the network.

11. The method of claim 9, comprising the further steps of:

determining the propagation time offset by sampling the signal of the original subscriber unit using a clock having a clock rate corresponding to a first resolution; and

providing the adjustment data at a second, coarser resolution.

12. The method of claim 11, wherein:

the clock rate is increased from a nominal level corresponding to said second resolution for recovering upstream transmissions from subscriber units in the network, to a higher level to achieve the first resolution for determining the propagation time offset.

13. The method of claim 11, wherein:

the clock rate operates at the first resolution for initially providing the adjustment data; and

the adjustment data is provided at the second resolution by omitting at least one least significant bit thereof.

14. The method of claim 11, wherein:

the clock rate operates at the first resolution for initially providing the adjustment data; and the adjustment data is provided at the second resolution by randomizing at least one least significant bit thereof.

15. The method of claim 1, wherein:

the recorded transmission characteristic comprises at least one of a frequency and a frequency offset.

16. The method of claim 15, comprising the further steps of:

providing adjustment data to adjust the frequency offset to a desired value; and

communicating the adjustment data to any subscriber unit in the network that uses an identifier associated with the original subscriber unit for use in adjusting a frequency thereof.

17. The method of claim 1, wherein:

the recorded transmission characteristic comprises at least one of a power and a power offset.

18. The method of claim 17, comprising the further steps of:

providing adjustment data to adjust the power offset to a desired value; and

communicating the adjustment data to any subscriber unit in the network that uses an identifier associated with the original subscriber unit for use in adjusting a power thereof.

19. The method of claim 1, wherein:

the recorded transmission characteristic comprises a spectral characteristic.

20. The method of claim 19, wherein:

the spectral characteristic comprises at least one of a power spectrum and a power spectrum offset.

21. The method of claim 20, comprising the further steps of:

providing adjustment data to adjust the power spectrum offset to a desired value; and

communicating the adjustment data to any subscriber unit in the network that uses an identifier associated with the original subscriber unit for use in adjusting a power spectrum thereof.

22. The method of claim 21, wherein:

the adjustment data comprises filter coefficient data.

23. The method of claim 1, wherein:

the recorded transmission characteristic is obtained from a measurement of the signal of the original subscriber unit.

24. An apparatus for detecting a clone subscriber unit in a communication network, comprising:

means for recording a transmission characteristic of a signal from an original subscriber unit that is authorized for use in said network;

means for measuring a comparable transmission characteristic of a signal from a subscriber unit on said network alleging to be said original subscriber unit; and

means determining whether there is a difference between the measured transmission characteristic and the recorded transmission characteristic;;

wherein any such difference is indicative that the alleging subscriber unit is a clone subscriber unit.

25. An apparatus for detecting a clone subscriber unit in a communication network, comprising:

means for recording a transmission characteristic of an original subscriber unit authorized for use in said network; and

means for comparing said recorded transmission characteristic to a comparable transmission characteristic of a subscriber unit on said network alleging to be said original subscriber unit;

wherein a difference between the compared transmission characteristics is indicative that the alleging subscriber unit is a clone subscriber unit.

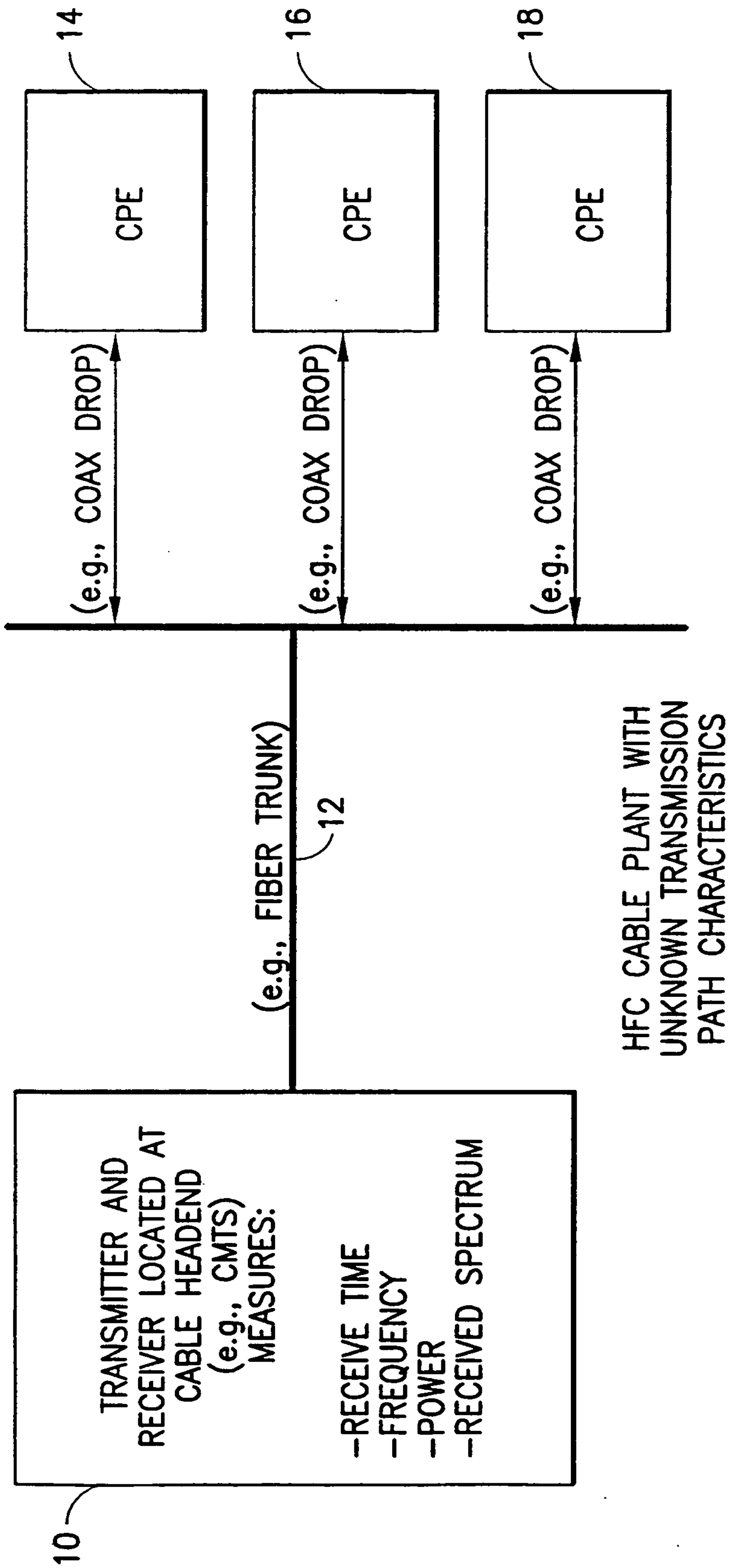

14
16
18
CPE
CPE
CPE
(e.g., COAX DROP)
(e.g., COAX DROP)
(e.g., COAX DROP)
(e.g., FIBER TRUNK)
12
HFC CABLE PLANT WITH UNKNOWN TRANSMISSION PATH CHARACTERISTICS
TRANSMITTER AND RECEIVER LOCATED AT CABLE HEADEND (e.g., CMTS) MEASURES:
-RECEIVE TIME
-FREQUENCY
-POWER
-RECEIVED SPECTRUM
10

FIG.1

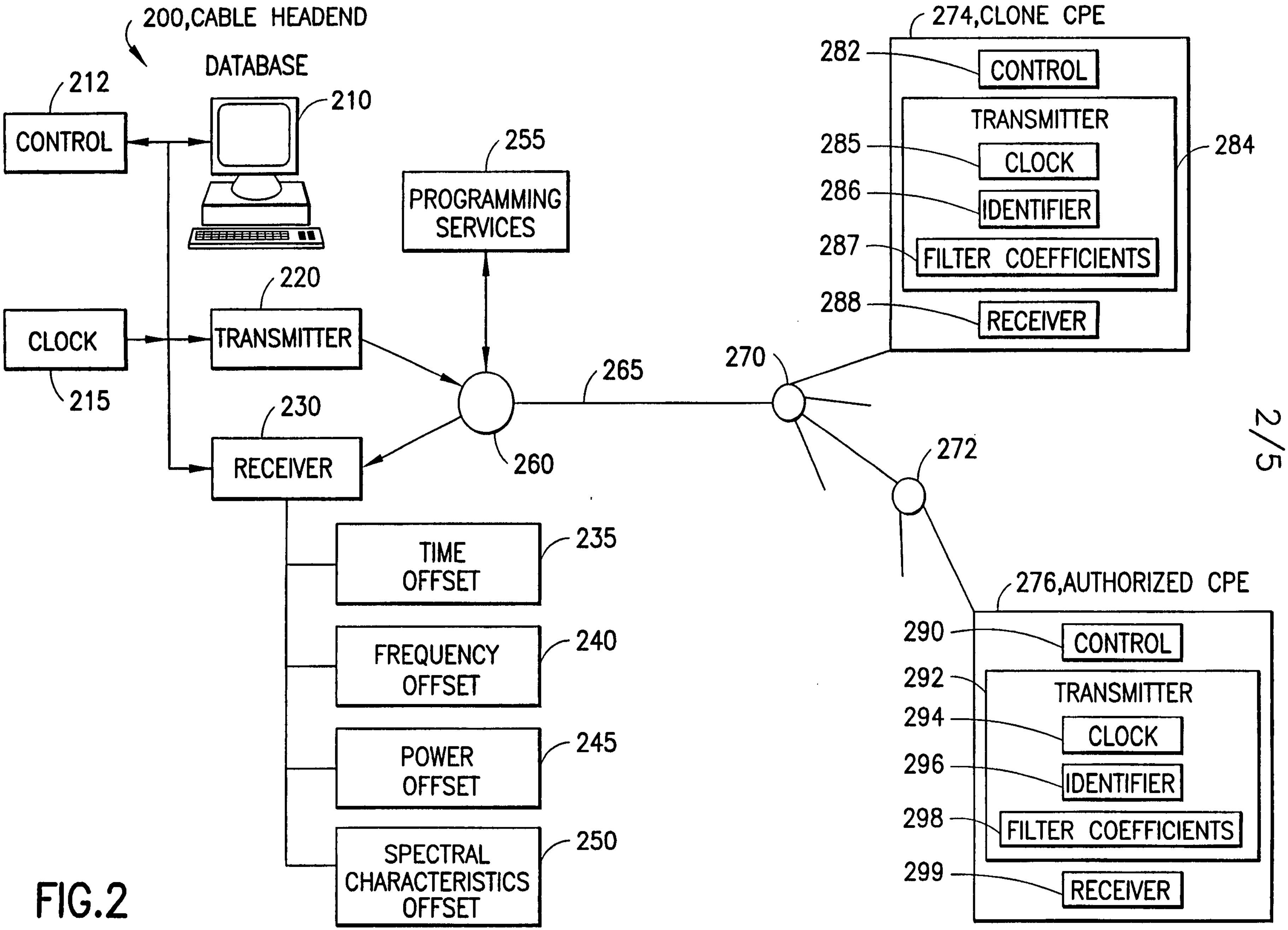

200,CABLE HEADEND
DATABASE
212
CONTROL
210
255
PROGRAMMING SERVICES
220
CLOCK
TRANSMITTER
215
230
RECEIVER
260
265
270
272
TIME OFFSET
235
FREQUENCY OFFSET
240
POWER OFFSET
245
SPECTRAL CHARACTERISTICS OFFSET
250
274,CLONE CPE
282
CONTROL
TRANSMITTER
284
285
CLOCK
286
IDENTIFIER
287
FILTER COEFFICIENTS
288
RECEIVER
276,AUTHORIZED CPE
290
CONTROL
292
TRANSMITTER
294
CLOCK
296
IDENTIFIER
298
FILTER COEFFICIENTS
299
RECEIVER

FIG.2

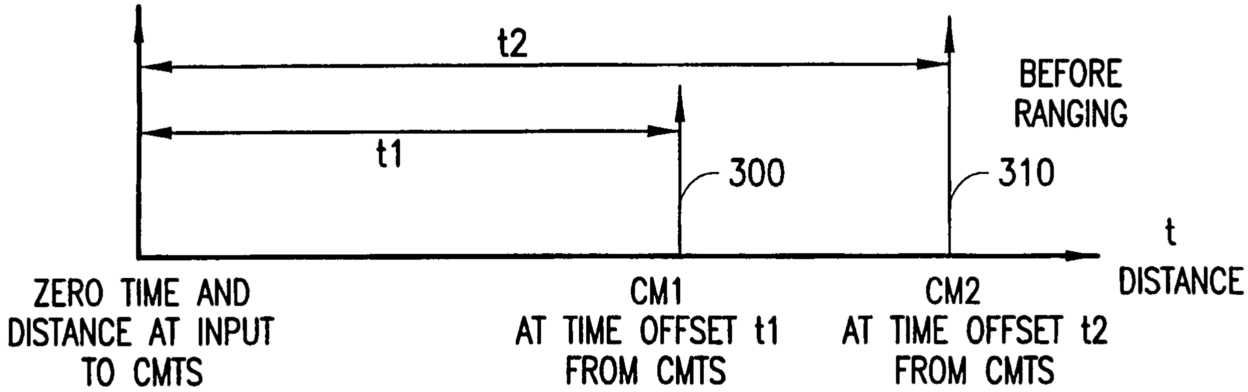

t2
t1
BEFORE RANGING
300
310
t
DISTANCE
ZERO TIME AND DISTANCE AT INPUT TO CMTS
CM1 AT TIME OFFSET t1 FROM CMTS
CM2 AT TIME OFFSET t2 FROM CMTS

FIG.3a

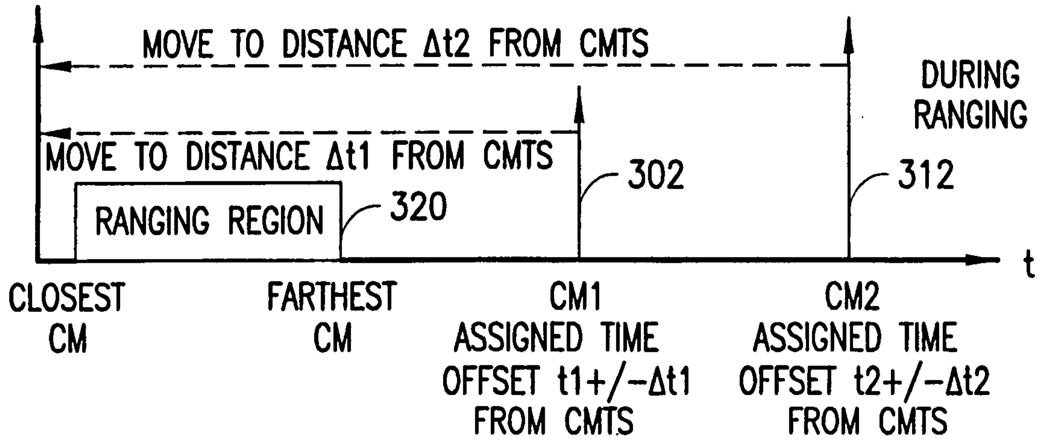

MOVE TO DISTANCE Δt2 FROM CMTS
DURING RANGING
MOVE TO DISTANCE Δt1 FROM CMTS
302
312
RANGING REGION
320
t
CLOSEST CM
FARTHEST CM
CM1 ASSIGNED TIME OFFSET t1+/-Δt1 FROM CMTS
CM2 ASSIGNED TIME OFFSET t2+/-Δt2 FROM CMTS

FIG.3b

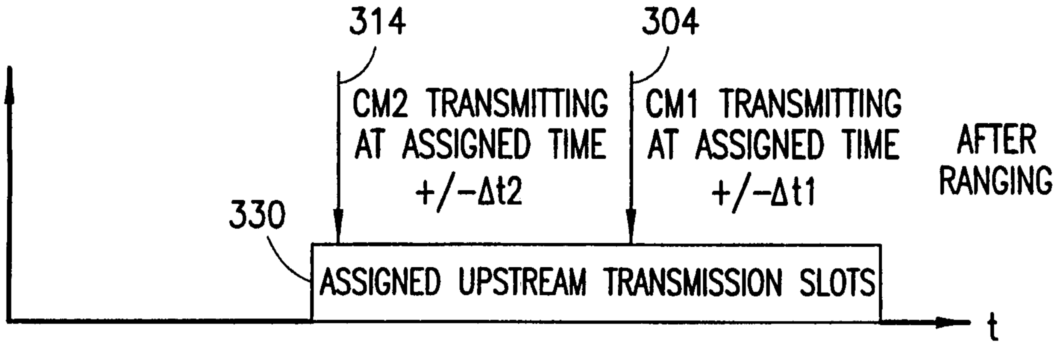

314
304
CM2 TRANSMITTING
AT ASSIGNED TIME
+/−Δt2
CM1 TRANSMITTING
AT ASSIGNED TIME
+/−Δt1
AFTER
RANGING
330
ASSIGNED UPSTREAM TRANSMISSION SLOTS
t

FIG.3c

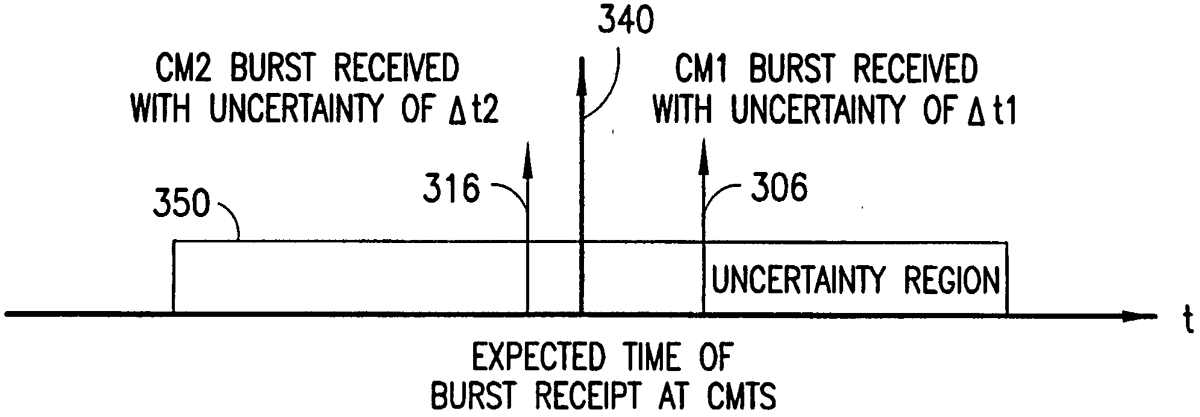

340
CM2 BURST RECEIVED
WITH UNCERTAINTY OF Δt2
CM1 BURST RECEIVED
WITH UNCERTAINTY OF Δt1
350
316
306
UNCERTAINTY REGION
t
EXPECTED TIME OF
BURST RECEIPT AT CMTS

FIG.3d

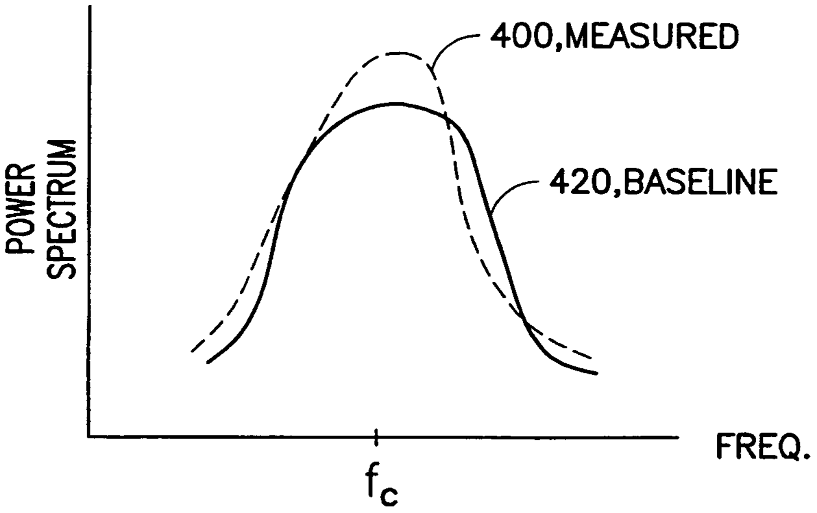


FIG.4

INTERNATIONAL SEARCH REPORT

Intei onal Application No
PCT/US 00/01021

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/173 H04N17/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N H04B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 335 265 A (SONBERG KENNETH W ET AL) 2 August 1994 (1994-08-02) column 1, line 59 -column 2, line 21 column 8, line 27 - line 61 table 1 figures 1-4 ---	1-3,7, 24,25
A	ELDERING C A ET AL: "CATV RETURN PATH CHARACTERIZATION FOR RELIABLE COMMUNICATIONS" IEEE COMMUNICATIONS MAGAZINE,US,IEEE SERVICE CENTER. PISCATAWAY, N.J, vol. 33, no. 8, 1 August 1995 (1995-08-01), pages 62-69, XP000525541 nEW yORK, ny, us ISSN: 0163-6804 --- -/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 28 April 2000	Date of mailing of the international search report 08/05/2000
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Van der Zaal, R

1

INTERNATIONAL SEARCH REPORT

Inter. onal Application No
PCT/US 00/01021

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 473 361 A (PENNEY BRUCE J) 5 December 1995 (1995-12-05) -----	

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 00/01021

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5335265 A	02-08-1994	DE 69227122 D	29-10-1998
		DE 69227122 T	25-03-1999
		EP 0611513 A	24-08-1994
		JP 7500955 T	26-01-1995
		WO 9309640 A	13-05-1993
US 5473361 A	05-12-1995	NONE	